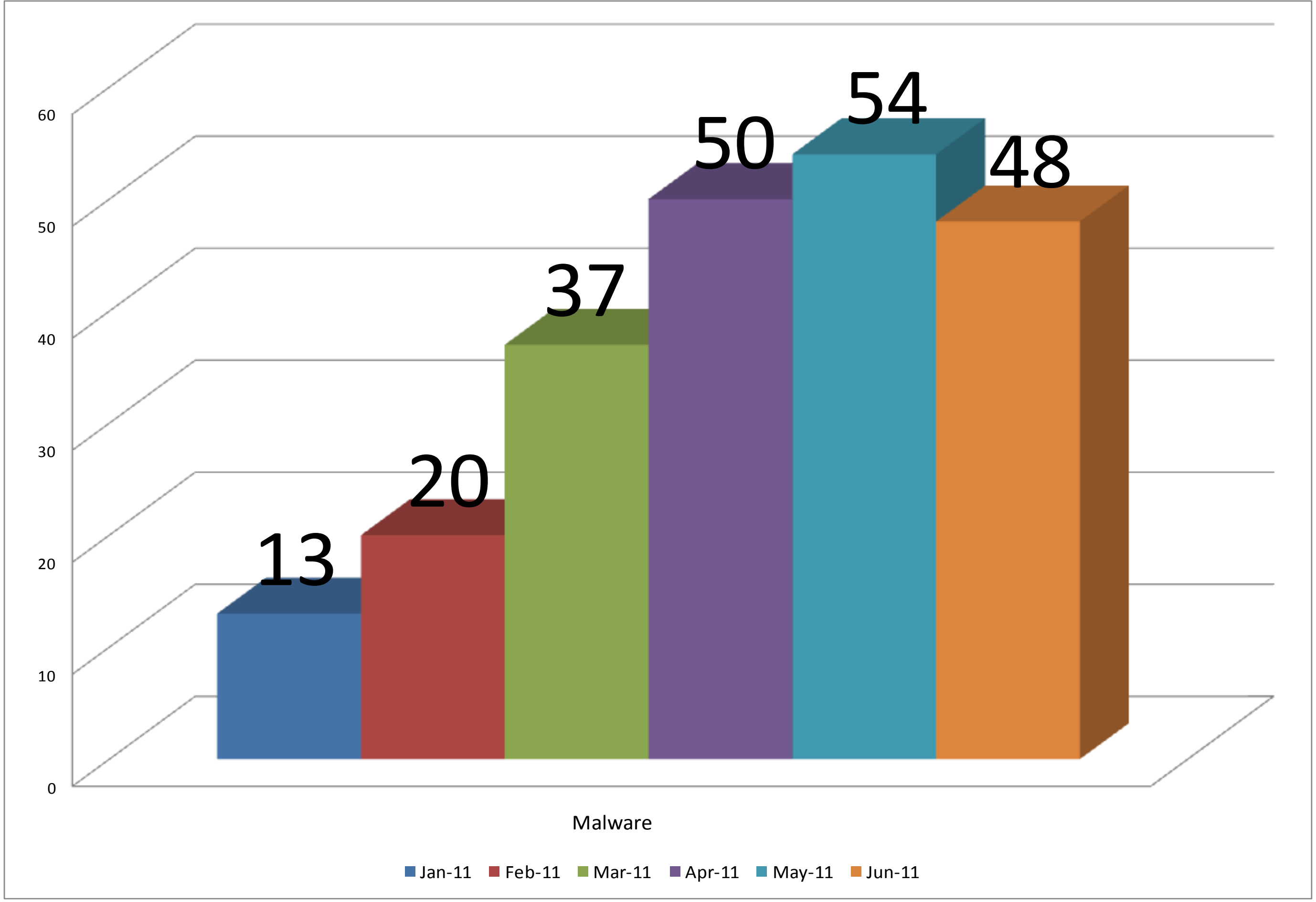
# Security and Java Update

Trey Stevens, Northrop Grumman
Michael Watson, VITA

AITR Meeting
Aug. 10, 2011

# Security Incident Trend



- The number of malware-related incidents more than doubled from the first quarter
- Malware is using vulnerabilities in Java JRE, Adobe Acrobat Reader and Adobe Flash

## Java and malware

Antivirus products only effectively detecting and cleaning 60 percent of the variants found; malware is starting to exhibit more malicious behavior

- Outbound network communication attempts
- Rootkit behavior
- Keystroke logging
- Data compromise attempts

# Complications with Java

- Is hardware *independent*
  - Write an application one time and run it across multiple operating systems
- Not all versions have the same functionality
  - Features and/or functions may have been removed for security reasons
  - Stability improvements may cause changes to the core Java programming
- Some applications are dependent upon a vendor-provided, specific customized version of Java

# Security Standard Requirements

- Three applicable sections in ITRM Standard SEC501-06 (Section 4.3. IT System Hardening)
  - 4.3. 2.9. Apply all software publisher security updates to the associated software products
  - 4.3. 2.10. All security updates must be applied as soon as possible after appropriate testing, not to exceed 90 days for implementation
  - 4.3. 2.11. Prohibit the use of software products that the software publisher has designated as end-of-life (i.e., software publisher no longer provides security patches for the software product)
- Agency ISO should follow Information Security exception process
  - ITRM Standard SEC501-06 Appendix – Information Security Policy and Standard Exception Request Form

# Recommendation

- Add Java to the centrally supported core image
- Have the latest version of Java installed
  - Browser points to latest version
- Applications point to old versions as needed
- Updates follow change control and are tested by agencies

# Other option

- Keep as an agency application
- Use the standard work request to make updates
- File a security exception when using other than the latest version

# Homework

- Should the JRE be part of the standard package that VITA provides?
  - Determine how your agency uses Java
  - See PARS information for what is in the environment
  - Review applications to see if they require older versions or if they depend on browser default
- Note: Both options require agencies to file security exceptions for software that is out of original equipment manufacturer support
- Provide feedback to customer account manager (CAM) by close of business Aug. 27 regarding concerns about adding Java to the standard image
- Do we need a technical call for Q&A before Aug. 27?